BILLING C

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2021-OS-0078]

Privacy Act of 1974; System of Records

AGENCY: Defense Information Systems Agency (DISA), Department of Defense (DoD).

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is modifying and reissuing a current system of records titled "Identity Synchronization Services (IdSS)," K890.14. This system of records was originally established by the DISA to populate and maintain persona-based user objects in DoD enterprise-level Domain Controllers, such as the Enterprise Application and Services Forest (EASF) implemented by DISA to provide DoD Enterprise E-Mail, DoD Enterprise Portal Service (DEPS), etc. In addition, the DISA uses the IdSS to populate and maintain persona data elements in DoD Component networks and systems, such as directory services and account provisioning systems. This system of records notice (SORN) is being updated to make various changes, including expanding the individuals covered and adding DoD's standard routine uses.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before **[INSERT 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].** The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

Federal Rulemaking Portal: https://www.regulations.gov.

Follow the instructions for submitting comments.

Mail: DoD cannot receive written comments at this time due to the COVID-19

pandemic. Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mrs. Jeanette M. Weathers-Jenkins, DISA Privacy Officer, 6914 Cooper Ave, Fort Meade, MD 20755-7090, or by phone at (301) 225-8158.

SUPPLEMENTARY INFORMATION:

I. Background

The DISA is modifying the K890.14 IdSS system of records, to provide DoD Enterprise E-Mail, DEPS, etc. In addition, it will allow the IdSS to populate and maintain persona data elements in DoD Component networks and systems, such as directory services and account provisioning systems to provide DoD Enterprise E-Mail. Subject to public comment, the DoD proposes to update this SORN to add the standard DoD routine uses (routine uses A through I) and to allow for additional disclosures outside DoD related to the purpose of this system of records.

Additionally, the following sections of this SORN are being modified as follows: (1) System Location and System Manager(s), to provide instructions on obtaining a list of system location(s); (2) Authority for Maintenance of the System, to update citation(s) and add additional authorities; (3) Purpose(s) of the System, to clarify the system's purpose for the general public; (4) Categories of Individuals Covered by the System, to expand the individuals covered, and Categories of Records, to clarify how the records relate to the revised Category of Individuals; (5) Record Source Categories, to provide clarity; (6) Routine Uses, to align with DoD's standard routine uses; (7) Record Access Procedures, to reflect the need for individuals to identify the

appropriate DoD office or component to which their request should be directed; and (8) Contesting Records Procedures and Notification Procedures, to update the appropriate citation for contesting records. Additionally, the sections containing the policies on storage, retrieval of records, retention and disposal of records, and safeguards have been modified to improve clarity generally and for compliance with National Archives and Records Administration approved records schedules. This notice also includes non-substantive changes to simplify the formatting and text of the previously published notice.

DoD SORNs have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD) website at https://dpcld.defense.gov/privacy.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DPCLTD has provided a report of this system of records to the OMB and to Congress.

Dated: July 26, 2021.

Aaron T. Siegel,

Alternate OSD Federal Register,

Liaison Officer,

Department of Defense.

SYSTEM NAME AND NUMBER: Identity Synchronization Services (IdSS), K890.14

SECURITY CLASSIFICATION: Unclassified

SYSTEM LOCATION: System locations may be obtained from the system manager at the Defense Information Systems Agency (DISA), Services Directorate, 6910 Cooper Ave., Fort Meade, MD 20755-7090.

SYSTEM MANAGER(S): Chief, Enterprise Directory Services, Defense Information Systems Agency (DISA), Services Directorate, Applications Division, Infrastructure Applications Branch, 6910 Cooper Ave., Fort Meade, MD 20755-7090, telephone number 301-225-9201, email: disa.meade.se.list.idss-product-management@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. Chapter 8, Defense Agencies and Department of Defense Field Activities; DoD Directive 5105.19, Defense Information Systems Agency (DISA); DoD Instruction (DoDI) 1000.25, DoD Personnel Identity Protection (PIP) Program; DoDI 5200.46, DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC); and DoDI 8520.03, Identity Authentication for Information Systems.

PURPOSE(S) OF THE SYSTEM:

A. To populate and maintain persona-based user objects in DoD enterprise-level Domain Controllers, such as the Enterprise Application Services Forest (EASF) implemented by DISA to provide DoD Enterprise E-Mail, DoD Enterprise Portal Service (DEPS), etc.

B. To populate and maintain persona data elements in DoD Component networks and systems, such as directory services and account provisioning systems to provide DoD Enterprise E-Mail.

C. To populate and maintain persona data elements in DoD Component (including the United States Coast Guard (USCG) networks and systems, such as directory services and account provisioning systems.

D. To utilize enterprise services to establish a reliable and uniform secure data portal for the transmittal of shared information between DoD and the U.S. Department of Veterans Affairs (VA).

E. To populate and maintain persona data elements to support continuous data exchange between DoD and its Coalition Partners and partner Five Eyes Nations to enable current and future information sharing capabilities that are used by the respective warfighters for conducting mission supporting operations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

A. DoD personnel, meaning those who have been issued DoD Common Access Cards (CAC) or a DoD Class 3 Public Key Infrastructure (PKI) certificate, to include civilian employees, military personnel, contractors and other individuals detailed or assigned to DoD Components.

B. VA Personal Identity Verification (PIV) card holders identified by the VA's Interagency Care Coordination Committee (IC3).

CATEGORIES OF RECORDS IN THE SYSTEM:

A. For DoD personnel: Individuals name, unique identifiers including DoD ID number, other unique identifier, Federal Agency Smart Credential Number (FASC-N), login name, legacy login name, and persona username, object class, rank, title, job title, persona type code (PTC), persona display name (PDN), address, e-mail, phone, and other contact information for work and home locations, non-US government agency object common name; user account control, information technology service entitlements, Unit Identification Code (UIC), and PKI certificate information. Administrative Organization Code, DoD component, DoD sub-component, Non-DoD agency, Directory publishing restrictions, Reserve Component Code, Billet Code, Pay Grade, type of investigation, date of investigation, and security clearance level.

B. For VA personnel: Individual's name, other unique identifier, primary and other work e-mail addresses, administrative organization code, duty sub-organization code persona e-mail address, e-mail encryption certificate, and driver's license number.

NOTE: This system does not collect or maintain the individual's Social Security Number.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: DoD Component directories such as the Defense Eligibility Enrollment Reporting System (DEERS), Person Data Repository (PDR) for DoD person and persona data, the DISA DoD PKI Global Directory Service (GDS) for user PKI email certificates, partner Five Eyes Nations, and the Coalition partners.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the

records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

J. To the USCG to share DoD information to ensure it maintains a state of readiness to function as a specialized military Service in the Department of Navy in a time of war or national emergency.

K. To DoD-approved Coalition Partners for the purposes of routine mission supporting activities.

L. To partner Five Eyes (FVEY) Nations to provide information pursuant to existing bilateral agreement(s) in order to populate the information into the FVEY national directory.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, or digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: These records are retrieved by individual name, DoD ID Number, or email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: System's sole function is to receive and integrate data from two or more other systems and export the resultant product to yet another independent system. These records are maintained as temporary which may be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Access to the type and amount of data is governed by privilege management software and policies developed and enforced by Federal government personnel. Data is protected by repository and interfaces, including, but not limited to multi-layered firewalls, Secure Sockets Layer/Transport Layer Security (SSL/TLS) connections, access control lists, file system permissions, intrusion detection and prevention systems and log monitoring. Complete access to all records is restricted to and controlled by certified system management personnel, who are responsible for maintaining the IdSS system integrity and the data confidentiality. Access to computerized data is restricted by CAC.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the FOIA Service Center, Defense Information Systems Agency, ATTN: Headquarters FOIA Requester Service Center, P.O. Box 549, Ft. Meade, MD 20755-0549. Signed, written requests should include the individual's full name, current address, telephone number, and the name and number of this system of records notice. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial Component determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: December 8, 2010, 75 FR 76428.

[FR Doc. 2021-16304 Filed: 7/29/2021 8:45 am; Publication Date: 7/30/2021]